CLAIMS

What is claimed is:

1. An apparatus for encrypting messages exchanged by a telecommunication's system communicating pair, the communicating pair comprising a first transmitter-receiver and a second transmitter-receiver, the apparatus having devices for sending cryptographic messages from the first transmitter-receiver to the second transmitter-receiver to be decrypted by the second transmitter-receiver, the apparatus comprising:

(a) a first storage device in the first transmitter-receiver for storing messages and previous transmissions, or parts thereof, the messages or transmissions previously sent to and received from the second transmitter-receiver of the pair;

(b) a second storage device for storing transmissions and messages or parts thereof, the transmissions and messages previously sent to and received from the first transmitter-receiver of the pair;

(c) a plurality of cryptographic devices in the first transmitter-receiver, each of the cryptographic devices having a reference known to the first transmitter-receiver;

(d) the same plurality of cryptographic devices with references also known to the second transmitter-receiver;

(e) a selection device in the first transmitter-receiver for selecting and retrieving a transmission or message or a part thereof previously sent to the second transmitter-receiver;

(f) a state computation device in the first transmitter-receiver for computing a random number as a function of a reference over one of the plurality of cryptographic devices known to the communicating pair, the function also being over a previous transmission or message sent to the second transmitter-receiver, the set of states known to the communicating pair;

(g) a message sending device in the first transmitter-receiver for creating and sending a message to the second transmitter-receiver, the message containing the a previously sent transmission or message, or some part thereof, sent by the first transmitter

receiver, and a reference to a transmission or message previously sent to the first transmitter-receiver by the second transmitter-receiver, the message sending device further encrypting the message using a cryptographic device randomly selected by the first transmitter-receiver;

(h) a message receiving device in the second transmitter-receiver for receiving the message sent by the first transmitter-receiver, the message receiving device also extracting the encrypted previous transmission or message or part thereof sent by the first transmitter-receiver, and further extracting the reference sent by the first transmitter-receiver;

(i) a cryptographic device reference decoder in the second transmitter-receiver for discovering the reference to the cryptographic device randomly selected by the first transmitter-receiver;

(j) a reference decoding device in the second transmitter-receiver for controlling the cryptographic device associated with the reference discovered by the cryptographic reference decoder, the cryptographic decoding device applying the referenced cryptographic device to decrypt the previous transmission or message or part thereof sent by the first transmitter-receiver and to decrypt the reference to a transmission or message previously sent by the second transmitter receiver;

(k) a message selection device in the second transmitter-receiver for selecting a previous transmission or message or a part thereof, stored in the second storage device, and for encrypting the transmission or message or a part thereof, selected, the message or part thereof encrypted using the encryption device associated with the reference discovered, and for sending the encrypted selected message or part thereof to the first transmitter-receiver; and

(l) a confirmation device in the first transmitter-receiver for confirming the correct reference was found by the second transmitter-receiver, and for confirming the correct transmission message previously sent by the second transmitter-receiver, the confirmation device using the cryptographic device associated with the cryptographic device reference sent to the second transmitter-receiver to decrypt the encrypted selected transmission or message sent by the second transmitter-receiver, and to evaluate the

contents of the decrypted selected transmission or message sent by the second transmitter-receiver and to signal confirmation of no-confirmation;

whereby the first transmitter-receiver, when sending an encrypted message to the second transmitter-receiver:

(a) randomly selects an encryption device associated with a reference, and randomly selects a reference to a transmission or message previously received from the second transmitter-receiver;

(b) using the randomly selected cryptographic device encrypts the previous transmission or message sent by the first transmitter-receiver and the reference to a previously sent by the second transmitter-receiver;

(c) sends the encrypted message to the second transmitter-receiver;

(d) the second transmitter-receiver discovers the cryptographic device randomly selected by the first transmitter-receiver and discovers the reference to the previous message sent;

(e) the second transmitter-receiver using the discovered encryption device encrypts the referenced transmission or message or some part thereof sent to the first transmitter-receiver, and sends the encrypted referenced transmission or message or part thereof the first transmitter-receiver; and

(f) the first transmitter-receiver confirms the correctness of the contents of the encrypted message sent by the second transmitter-receiver and confirms the security of a transmission to the second transmitter-receiver.